What is claimed is:

1. A method for authenticating the identity of a user by an authority, comprising:

enrolling at least one credential for the user with the authority;

establishing at least one shared secret between the user and the authority relating to a predefined shared secret manner for presenting a current user credential to the authority;

receiving at least one currently presented user credential by the authority for authentication of the identity of the user; and

authenticating the identity of the user by the authority based on a correspondence between the enrolled and current user credentials and a correspondence between the shared secret manner for presenting the current user credential and the manner in which the current user credential is presented to the authority.

2. The method of claim 1, wherein enrolling the user credential further comprises receiving the user credential by the authority for enrollment.

3. The method of claim 2, wherein receiving the user credential for enrollment further comprises storing the user credential by the authority.

4. The method of claim 3, wherein storing the user credential further comprises storing at least one biometric template for the user.

5. The method of claim 3, wherein storing the user credential further comprises storing a document for the user.

6. The method of claim 3, wherein storing the user credential further comprises storing the user credential on one of a host computer, a local terminal, and a smart card for the user.

7. The method of claim 1, wherein enrolling the user credential further comprises enrolling at least one biometric template and at least one document for the user.

8. The method of claim 7, wherein enrolling the biometric template further comprises enrolling the biometric template for at least one of a fingerprint template, a face template, a voice template, and an iris template for the user.

9. The method of claim 7, wherein enrolling the document further comprises enrolling at least one of a digital document and a paper document for the user.

10. The method of claim 9, wherein enrolling the digital document further comprises enrolling at least one of a digital certificate and a digital signature for the user.

11. The method of claim 9, wherein enrolling the paper document further comprises enrolling a passport for the user.

12. The method of claim 1, wherein enrolling the user credential with the authority further comprises storing user authentication information on a user token for the user.

13. The method of claim 12, wherein storing the information on the user token further comprises storing the user authentication information on a smart card for the user.

14. The method of claim 13, wherein storing the information on the smart card further comprises storing biometric information for the user.

15. The method of claim 14, wherein storing the biometric information for the user further comprises storing biometric information for one of a fingerprint, a face, a voice, and an iris for the user.

16. The method of claim 13, wherein storing the information on the smart card further comprises storing the shared secret for the user on the smart card.

17. The method of claim 13, wherein storing the information on the smart card further comprises storing the authentication information on the smart card signed with a private key for the user.

18. The method of claim 1, wherein enrolling the user credential further comprises enrolling at least one additional credential for the user with the authority.

19. The method of claim 1, wherein establishing the predefined shared secret manner of presenting the user credential further comprises establishing at least one predefined shared secret sequence of presenting the current user credential to the authority.

20. The method of claim 19, wherein establishing the predefined shared secret sequence of presenting the current user credential further comprises establishing the predefined shared secret sequence which functions in a manner analogous to a personal identification number for the user.

21. The method of claim 1, wherein establishing the shared secret further comprises storing information about the shared secret by the authority.

22. The method of claim 21, wherein storing the information about the shared secret by the authority further comprises storing the information about the shared secret and the user credential together in a database by the authority.

23. The method of claim 22, wherein storing the information about the shared secret and the user credential in the database further comprises storing the information about the shared secret and the user credential encrypted and digitally signed.

24. The method of claim 1, wherein establishing the shared secret further comprising establishing at least one additional shared secret between the user and the authority.

25. The method of claim 24, wherein establishing the additional shared secret further comprises establishing a predefined shared secret personal identification number for the user.

26. The method of claim 24, wherein establishing the additional shared secret further comprises establishing at least one additional predefined shared secret manner of presenting the current user credential to the authority for the user.

27. The method of claim 24, wherein establishing the additional shared secret further comprises establishing a predefined shared secret manner of presenting at least one additional current user credential to the authority for the user.

28. The method of claim 24, wherein establishing the additional shared secret further comprises establishing a predefined shared secret manner of presenting each of a plurality of additional current user credentials to the authority for the user.

29. The method of claim 28, wherein establishing the predefined shared secret manner of presenting of each of the plurality of additional current user credentials further comprises establishing a variation of the predefined shared secret manner of presenting each of the additional current user credentials to the authority for the user corresponding to a variation in a degree of security.

30. The method of claim 28, wherein establishing the predefined shared secret manner of presenting each of the plurality of additional current user credentials further comprises establishing a variation of the predefined shared secret manner of presenting each of the additional current user to the authority for the user for consecutive occasions.

31. The method of claim 1, wherein receiving the currently presented user credential further comprises receiving the current user credential by the authority in a predefined shared secret sequence.

32. The method of claim 1, wherein receiving the currently presented user credential further comprises receiving a current biometric sample by the authority.

33. The method of claim 32, wherein receiving the current biometric sample by the authority further comprises receiving a current biometric sample for one of a fingerprint, a face, a voice, and an iris for the user.

34. The method of claim 1, wherein receiving the currently presented user credential further comprises receiving the current user credential by the authority from the user in a shared secret manner directed by the authority.

35. The method of claim 34, wherein receiving the current user credential in the manner directed by the authority further comprises directing the user by the authority to present a biometric sample for at least one user fingerprint.

36. The method of claim 34, wherein receiving the current user credential in the manner directed by the authority further comprises directing the user by the authority to present a combination of biometric samples for at least two of a user fingerprint, a user face, a user voice, and a user iris in a predefined shared secret sequence.

37. The method of claim 1, wherein receiving the current user credential further comprises receiving at least one additional currently presented user credential by the authority.

38. The method of claim 37, wherein receiving the current user credential further comprises receiving at least one additional currently presented user credential by the authority in a manner directed by the authority.

39. The method of claim 37, wherein receiving the current user credential further comprises receiving at least one additional currently presented user credential by the authority in one of a plurality of randomly selected predefined shared secret sequences as directed by the authority.

40. The method of claim 1, wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user by one of a host computer and a local device.

41. The method of claim 40, wherein authenticating the identity of the user by the local device further comprises authenticating the identity of the user for activation one of a gate controller, a door opener, a telephone, and an appliance.

42. The method of claim 1, wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user based on the enrolled user credential and the shared secret manner for presenting

the current user credential stored together in one of a local database and a remote database of the authority.

43. The method of claim 1, wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user in order for access to one of a device, a physical location, and a network.

44. The method of claim 1, wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user to a smart card.

45. The method of claim 1, wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user to activate a silent alarm for the user.

46. A system for authenticating the identity of a user by an authority, comprising:

means for enrolling at least one credential for the user with the authority;

means for establishing at least one shared secret between the user and the authority relating to a predefined shared secret manner for presenting a current user credential to the authority;

means for receiving at least one currently presented user credential by the authority for authentication of the identity of the user; and

means for authenticating the identity of the user by the authority based on a correspondence between the enrolled and current user credentials and a correspondence between the shared secret manner for presenting the current user credential and the manner in which the current user credential is presented to the authority.

47. The system of claim 46, wherein the means for enrolling the user credential further comprises means for receiving the user credential by the authority for enrollment.

48. The system of claim 47, wherein the means for receiving the user credential for enrollment further comprises means for storing the user credential by the authority.

49. The system of claim 48, wherein the means for storing the user credential further comprises means for storing at least one biometric template for the user.

50. The system of claim 48, wherein the means for storing the user credential further comprises means for storing a document for the user.

51. The system of claim 483, wherein the means for storing the user credential further comprises means for storing the user credential on one of a host computer, a local terminal, and a smart card for the user.

52. The system of claim 46, wherein the means for enrolling the user credential further comprises means for enrolling at least one biometric template and at least one document for the user.

53. The system of claim 52, wherein the means for enrolling the biometric template further comprises means for enrolling the biometric template for at least one of a fingerprint template, a face template, a voice template, and an iris template for the user.

54. The system of claim 52, wherein the means for enrolling the document further comprises means for enrolling at least one of a digital document and a paper document for the user.

55. The system of claim 54, wherein the means for enrolling the digital document further comprises means for enrolling at least one of a digital certificate and a digital signature for the user.

56. The system of claim 54, wherein the means for enrolling the paper document further comprises means for enrolling a passport for the user.

57. The system of claim 46, wherein the means for enrolling the user credential with the authority further comprises means for storing user authentication information on a user token for the user.

58. The system of claim 57, wherein the means for storing the information on the user token further comprises means for storing the user authentication information on a smart card for the user.

59. The system of claim 58, wherein the means for storing the information on the smart card further comprises means for storing biometric information for the user.

60. The system of claim 59, wherein the means for storing the biometric information for the user further comprises means for storing biometric information for one of a fingerprint, a face, a voice, and an iris for the user.

61. The system of claim 58, wherein the means for storing the information on the smart card further comprises means for storing the shared secret for the user on the smart card.

62. The system of claim 58, wherein the means for storing the information on the smart card further comprises means for storing the authentication information on the smart card signed with a private key for the user.

63. The system of claim 46, wherein the means for enrolling the user credential further comprises means for enrolling at least one additional credential for the user with the authority.

64. The system of claim 46, wherein the means for establishing the predefined shared secret manner of presenting the user credential further comprises means for establishing at least one predefined shared secret sequence of presenting the current user credential to the authority.

65. The system of claim 64, wherein the means for establishing the predefined shared secret sequence of presenting the current user credential further comprises means for establishing the predefined shared secret sequence which functions in a manner analogous to a personal identification number for the user.

66. The system of claim 46, wherein the means for establishing the shared secret further comprises means for storing information about the shared secret by the authority.

67. The system of claim 66, wherein the means for storing the information about the shared secret by the authority further comprises means for storing the information about the shared secret and the user credential together in a database by the authority.

68. The system of claim 67, wherein the means for storing the information about the shared secret and the user credential in the database further comprises means for storing the information about the shared secret and the user credential encrypted and digitally signed.

69. The system of claim 46, wherein the means for establishing the shared secret further comprising establishing at least one additional shared secret between the user and the authority.

70. The system of claim 69, wherein the means for establishing the additional shared secret further comprises means for establishing a predefined shared secret personal identification number for the user.

71. The system of claim 69, wherein the means for establishing the additional shared secret further comprises means for establishing at least one additional predefined shared secret manner of presenting the current user credential to the authority for the user.

72. The system of claim 69, wherein the means for establishing the additional shared secret further comprises means for establishing a predefined shared secret manner of presenting at least one additional current user credential to the authority for the user.

73. The system of claim 69, wherein the means for establishing the additional shared secret further comprises means for establishing a predefined shared secret manner of presenting each of a plurality of additional current user credentials to the authority for the user.

74. The system of claim 73, wherein the means for establishing the predefined shared secret manner of presenting of each of the plurality of additional current user credentials further comprises means for establishing a variation of the predefined shared secret manner of presenting each of the

additional current user credentials to the authority for the user corresponding to a variation in a degree of security.

75. The system of claim 73, wherein the means for establishing the predefined shared secret manner of presenting each of the plurality of additional current user credentials further comprises means for establishing a variation of the predefined shared secret manner of presenting each of the additional current user to the authority for the user for consecutive occasions.

76. The system of claim 46, wherein the means for receiving the currently presented user credential further comprises means for receiving the current user credential by the authority in a predefined shared secret sequence.

77. The system of claim 46, wherein the means for receiving the currently presented user credential further comprises means for receiving a current biometric sample by the authority.

78. The system of claim 77, wherein the means for receiving the current biometric sample by the authority further comprises means for receiving a current biometric sample for one of a fingerprint, a face, a voice, and an iris for the user.

79. The system of claim 46, wherein the means for receiving the currently presented user credential further comprises means for receiving the current user credential by the authority from the user in a shared secret manner directed by the authority.

80. The system of claim 79, wherein the means for receiving the current user credential in the manner directed by the authority further comprises means for directing the user by the authority to present a biometric sample for at least one user fingerprint.

81. The system of claim 79, wherein the means for receiving the current user credential in the manner directed by the authority further comprises means for directing the user by the authority to present a combination of biometric samples for at least two of a user fingerprint, a user face, a user voice, and a user iris in a predefined shared secret sequence.

82. The system of claim 46, wherein the means for receiving the current user credential further comprises means for receiving at least one additional currently presented user credential by the authority.

83. The system of claim 82, wherein the means for receiving the current user credential further comprises means for receiving at least one additional currently presented user credential by the authority in a manner directed by the authority.

84. The system of claim 82, wherein the means for receiving the current user credential further comprises means for receiving at least one additional currently presented user credential by the authority in one of a plurality of randomly selected predefined shared secret sequences as directed by the authority.

85. The system of claim 46, wherein the means for authenticating the identity of the user by the authority further comprises means for authenticating the identity of the user by one of a host computer and a local device.

86. The system of claim 85, wherein the means for authenticating the identity of the user by the local device further comprises means for authenticating the identity of the user for activation one of a gate controller, a door opener, a telephone, and an appliance.

87. The system of claim 46, wherein the means for authenticating the identity of the user by the authority further comprises means for authenticating the identity of the user based on the enrolled user credential and the shared secret manner for presenting the current user credential stored together in one of a local database and a remote database of the authority.

88. The system of claim 46, wherein the means for authenticating the identity of the user by the authority further comprises means for authenticating the identity of the user in order for access to one of a device, a physical location, and a network.

89. The system of claim 46, wherein the means for authenticating the identity of the user by the authority further comprises means for authenticating the identity of the user to a smart card.

90. The system of claim 46, wherein the means for authenticating the identity of the user by the authority further comprises means for authenticating the identity of the user to activate a silent alarm for the user.

91. A method for authenticating the identity of a user by an authority, comprising:

enrolling a plurality of credentials for the user with the authority;

establishing a shared secret between the user and the authority relating to a predefined shared secret manner of presenting a current user credential corresponding to each of the plurality of enrolled user credentials;

receiving a presentment of at least one current user credential by the authority for authentication of the identity of the user; and

authenticating the identity of the user by the authority based on a correspondence between the enrolled and current user credentials and a correspondence between the shared secret manner for presenting the current user credential and the manner in which the current user credential is presented to the authority.